JWT

JSON Web Token

Qu'est-ce qu'un token ?

- **Facteur d'authentification de possession** (on **possède** un token mais on ne le connait pas par cœur...)
- Généralement associé à un ensemble de permissions dont dispose un utilisateur (de par son rôle ou ses informations)

Pourquoi privilégier le token au mot de passe ?

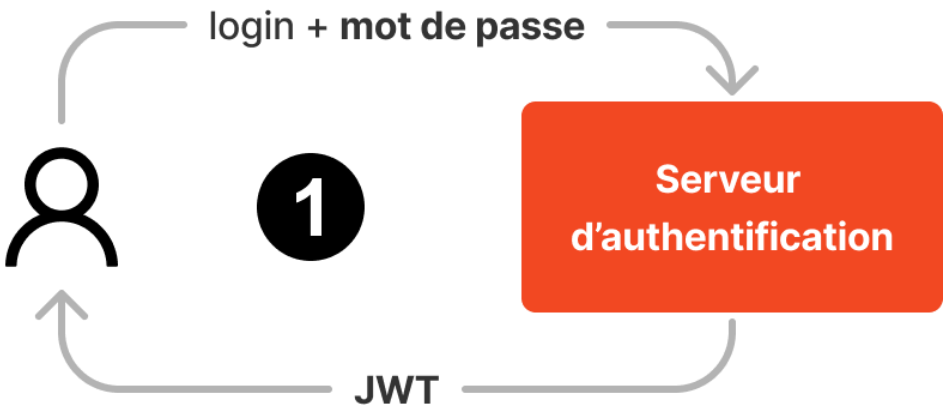
- Créer plusieurs token qui ont des **ensembles** de permissions différents
- Si un token est compromis, seules les permissions associées sont compromises
  - À l'inverse, si un mot de passe utilisateur est compromis, c'est **l'ensemble** des permissions liées à cet utilisateur qui sont compromises

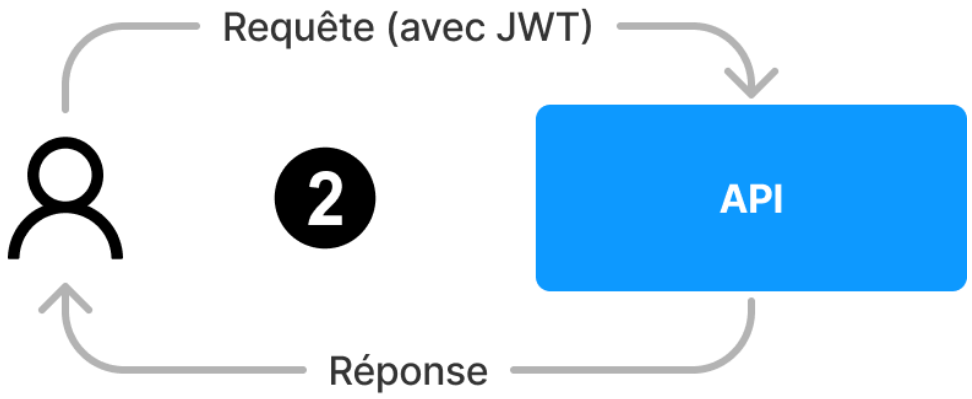
Clé d'API (API key)

- Une clé d'API est un type de token permettant d'accéder à une ressource
- Ce token fait office de **clé** permettant de "déverrouiller" l'accès à une API

JWT (JSON Web Token)

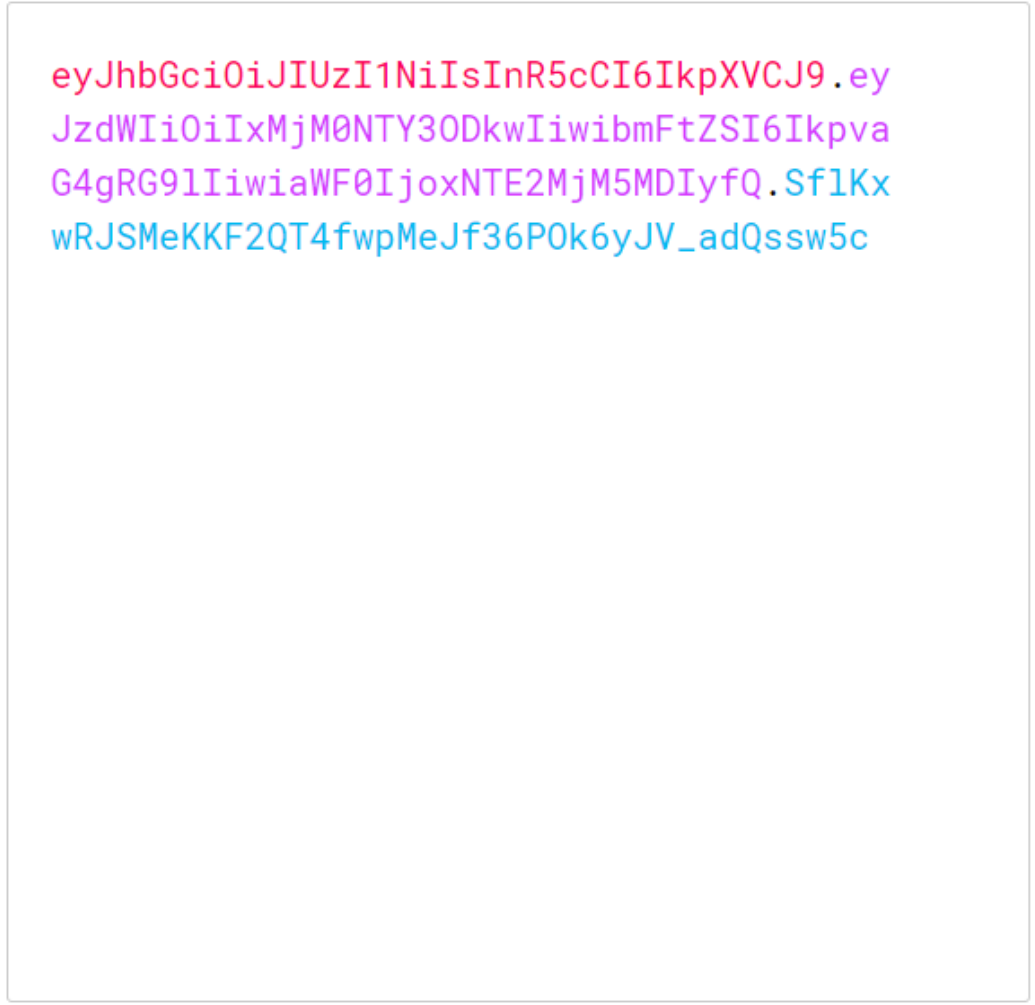
- RFC 7519: JSON Web Token (JWT)
- **Standard** très largement utilisé dans l'authentification sur le Web
- Simple à utiliser

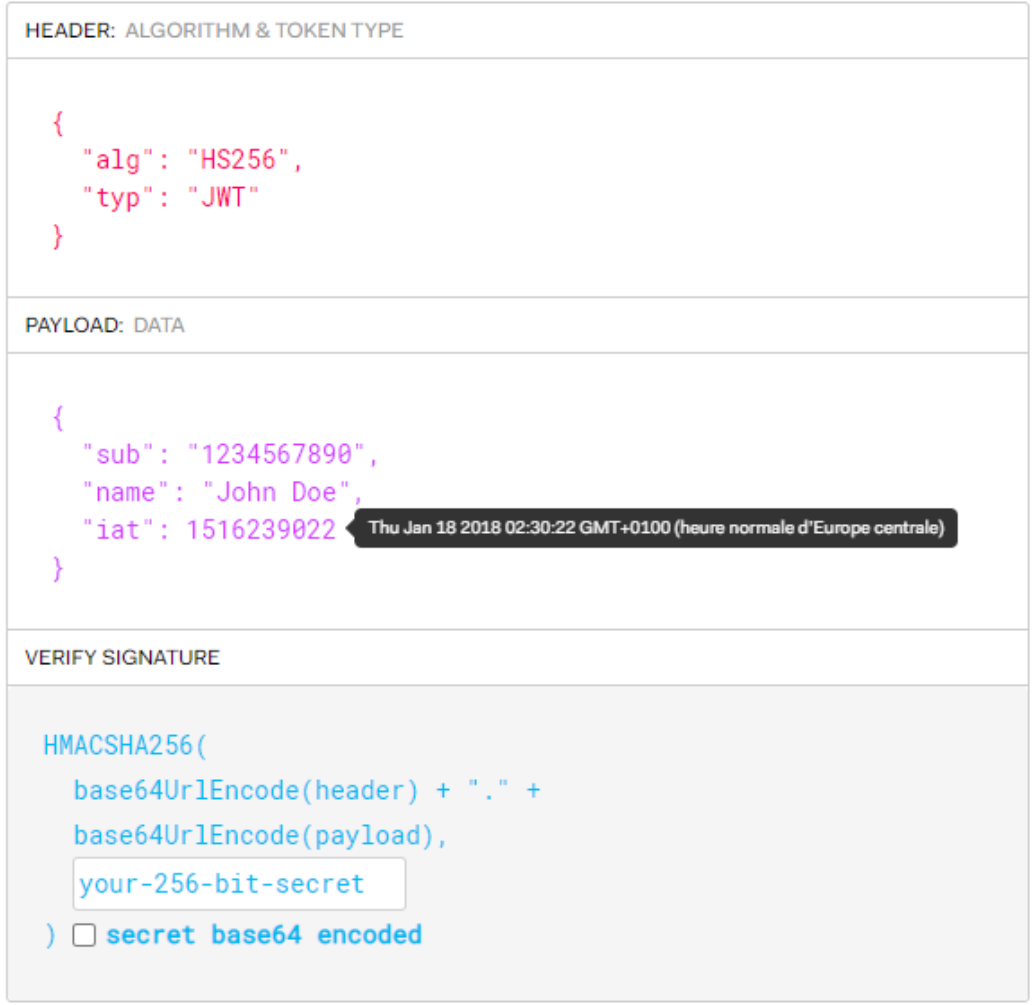




Fonctionnement du JWT

https://jwt.io/





Confiance

- Comment **authentifier** un JWT ?
- Grâce à un système **crypto** de **signature** (HMAC)